ABSTRACT

A method for enabling strong mutual authentication between two computers or devices in a communication system. A user attempting to gain access to a first computer transmits login information over a first communication channel to the first computer. The first computer transmits a first message, which in one embodiment includes a first key encrypted by a second key, to the second computer over the first communication channel. The first computer then transmits a second message to a third device over a second communication channel. The second message includes the second key needed by the second computer to decrypt the first message. The third device uses the user's login information to obtain the user's private key, which the third device uses to obtain the second key.

The third device transmits the second key in a third message to the second computer over a third communication channel. The second computer then uses the second key to decrypt the first message and obtain the first key.

Once the second computer obtains the first key, in one embodiment the second computer switches the role of the keys from the first message by encrypting the second key with the first key into a fourth message. The second computer transmits the fourth message to the server over the first communication channel, and the first computer decrypts the fourth message using its first key. If the received second key is the same as the generated second key, the second computer is authenticated to the first computer.